AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for re-encrypting encrypted data in a secure storage file system, comprising:

obtaining selected encrypted data ~~to re-encrypt~~ from the secure storage file system using a user data access record ~~and the encrypted data~~, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a [[new]] second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the [[new]] second symmetric key using [[a]] the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if ~~the public key is associated with~~ a ~~file system~~ second user ~~having~~ has read permission, wherein the second user is allowed access to the private key; and

storing an encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the ~~file system~~ second user has write permission.

2. (Currently Amended) The method of claim 1, wherein the user data access record comprises at least one selected from the group consisting of ~~a bitmap,~~ a bitmap for each user[[,]] and a bitmap for each group of users.

3. (Original) The method of claim 1, wherein the write permission comprises at least one sub-division.

4. (Original) The method of claim 3, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

5. (Original) The method of claim 1, wherein the secure storage file system is implemented using a preloaded shared library.

6. (Original) The method of claim 5, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

7. (Original) The method of claim 1, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

8. (Currently Amended) A method for re-encrypting a plurality of layer-encrypted data blocks in a secure storage file system, comprising:

obtaining at least one of the plurality of layer-encrypted data blocks from the secure storage file system ~~to re-encrypt~~ using a user data access record ~~and the plurality of layer-encrypted data blocks~~, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a user;

decrypting the at least one of the plurality of layer-encrypted data blocks using a first layer key; and

re-encrypting the at least one of the plurality of layer-encrypted data blocks using a [[new]] second layer key to obtain a new layer-encrypted data block.

9. (Currently Amended) The method of claim 8, wherein the user data access record comprising at least one selected from the group consisting of ~~a bitmap,~~ a bitmap for each user[[,]] and a bitmap for each group of users.

10. (Original) The method of claim 8, wherein the at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key and encrypted data.

11. (Original) The method of claim 8, wherein the at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key, an encrypted hash data, and encrypted data.

12. (Original) The method of claim 8, wherein the first layer key and the [[new]] second layer key are provided by an authentication agent.

13. (Currently Amended) A computer system generating a secure storage file system, comprising:

a processor;

a memory;

a storage device;

a computer display; and

software instructions stored in the memory for enabling the computer system under control of the processor, to perform:

obtaining selected encrypted data ~~to re-encrypt~~ from the secure storage file system using a user data access record ~~and the encrypted data~~, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a [[new]] second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the [[new]] second symmetric key using [[a]] the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if ~~the public key is associated with~~ a ~~file system~~ second user ~~having~~ has read permission, wherein the second user is allowed access to the private key; and

storing an encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the ~~file system~~ second user has write permission.

14. (Original) The computer system of claim 13, wherein the write permission comprises at least one sub-division.

15. (Currently Amended) The computer system of claim [[15]] 14, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

16. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a preloaded shared library.

17. (Original) The computer system of claim 16, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

18. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

19. (Currently Amended) The computer system of claim 13, wherein the user data access record comprises at least one selected from the group consisting of ~~a bitmap,~~ a bitmap for each user and a bitmap for each group of users.

20. (Currently Amended) A secure storage system comprising:

a storage provider storing encrypted data, wherein re-encrypting the encrypted data comprises:

obtaining selected encrypted data ~~to re-encrypt~~ from the secure storage file system executing on the storage provider using a user data access record ~~and the encrypted data based on receipt of~~ in response to receiving a key re-encryption event, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the selected encrypted data using a first symmetric key to obtain selected data;

re-encrypting the selected data using a [[new]] second symmetric key to obtain new encrypted data;

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the [[new]] second symmetric key using [[a]] the public key to obtain a new encrypted symmetric key;

storing the new encrypted data and the new encrypted symmetric key if ~~the public key is associated with~~ a ~~file system~~ second user ~~having~~ has read permission, wherein the second user is allowed access to the private key; and

storing an encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the ~~file system~~ second user has write permission; and

a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the encrypted data.

21. (Currently Amended) The system of claim 20, wherein the user data access record comprises at least one selected from the group consisting of ~~a bitmap,~~ a bitmap for each user[[,]] and a bitmap for each group of users.

22. (Original) The system of claim 20, wherein the write permission comprises at least one sub-division.

23. (Original) The system of claim 22, wherein the sub-division is selected from a group consisting of append, truncate, and delete.

24. (Currently Amended) A secure storage system comprising:

a storage provider storing a plurality of layer-encrypted data blocks, wherein re-encrypting layer-encrypted data blocks comprises:

obtaining at least one of the plurality of layer-encrypted data blocks ~~to re-encrypt~~ from the secure storage file system executing on the storage provider using a user data access record ~~and the plurality of layer-encrypted data blocks based on receipt of~~ in response to receiving a key re-encryption event, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

decrypting the at least one of the plurality of layer-encrypted data blocks using a first layer key; and

re-encrypting the at least one of the plurality of [[one]] layer-encrypted data blocks using a [[new]] second layer key to obtain a new layer-encrypted data block; and

a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the plurality of layer-encrypted data blocks.

25. (Currently Amended) The system of claim 24, wherein the user data access record comprises at least one selected from the group consisting of ~~a bitmap,~~ a bitmap for each user[[,]] and a bitmap for each group of users.

26. (Currently Amended) The system of claim 24, wherein [[of]] the ~~plurality of~~ at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key and encrypted data.

27. (Currently Amended) The system of claim 24, wherein the at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key, an encrypted hash data, and encrypted data.

28. (Currently Amended) The system of claim 24, wherein the first layer key and the [[new]] second layer key [[is]] are provided by an authentication agent.

29. (Currently Amended) An apparatus for re-encrypting a plurality of layer-encrypted data blocks in a secure storage file system, comprising:

means for obtaining at least one of the plurality of [[one]] layer-encrypted data blocks ~~to re-encrypt~~ from a secure storage file system using a user data access ~~record and the plurality layer-encrypted data blocks~~, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a user;

means for decrypting the at least one of the plurality of layer-encrypted data blocks using a first layer key; and

means for re-encrypting the at least one of the plurality of layer-encrypted data blocks using a [[new]] second layer key to obtain a new layer-encrypted data block.

30. (Currently Amended) An apparatus for re-encrypting encrypted data in a secure storage file system, comprising:

means for obtaining selected encrypted data ~~to re-encrypt~~ from a secure storage file system using a user data access record ~~and the encrypted data~~, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;

means for decrypting the selected encrypted data using a first symmetric key to obtain selected data;

means for re-encrypting the selected data using a [[new]] second symmetric key to obtain new encrypted data;

means for obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

means for encrypting the [[new]] second symmetric key using [[a]] the public key to obtain a new encrypted symmetric key;

means for storing the new encrypted data and the new encrypted symmetric key if ~~the public key is associated with~~ a ~~file system~~ second user ~~having~~ has read permission, wherein the second user is allowed access to the private key; and

means for storing an encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the ~~file system~~ second user has write permission.